Netmon

1. Scan

```
nmap -T4 -p- -A 10.10.10.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-18 14:04 EDT
Nmap scan report for 10.10.10.152
Host is up (0.047s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19  12:18AM                1024 .rnd
| 02-25-19  10:15PM       <DIR>          inetpub
| 07-16-16  09:18AM       <DIR>          PerfLogs
| 02-25-19  10:56PM       <DIR>          Program Files
| 02-03-19  12:28AM       <DIR>          Program Files (x86)
| 02-03-19  08:08AM       <DIR>          Users
|_02-25-19  11:49PM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
```

49669/tcp open msrpc   Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 11m11s, deviation: 0s, median: 11m11s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_   Message signing enabled but not required
| smb2-time:
| date: 2021-06-18T18:23:00
|_ start_date: 2021-06-18T18:14:31

TRACEROUTE (using port 1723/tcp)
HOP RTT   ADDRESS
1   48.73 ms 10.10.14.1
2   48.78 ms 10.10.10.152

Enum

Port 21 - FTP

https://www.howtoforge.com/tutorial/how-to-use-ftp-on-the-linux-shell/

https://www.offensive-security.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/

- Enum the FTP server

```
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19  11:44PM       <DIR>          Administrator
02-03-19  12:35AM       <DIR>          Public
226 Transfer complete.
ftp> cd Public
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  08:05AM       <DIR>          Documents
07-16-16  09:18AM       <DIR>          Downloads
07-16-16  09:18AM       <DIR>          Music
07-16-16  09:18AM       <DIR>          Pictures
02-03-19  12:35AM                   33 user.txt
07-16-16  09:18AM       <DIR>          Videos
```

- Download to our machine

1. Setup directory

→ lcd /root/Downloads

```
ftp> lcd /root/Downloads
Local directory now /root/Downloads
```

→

```
┌──(root💀kali)-[~]
└─# cd Downloads

┌──(root💀kali)-[~/Downloads]
└─# ls
black-box-penetration-test-1.ovpn  lab_tsunam1.ovpn                      webshell.war
cmd.war                            Nessus-8.13.2-ubuntu910_amd64.deb     windowhaha
config.old                         perl-reverse-shell-1.0
image.jpeg                         user.txt

┌──(root💀kali)-[~/Downloads]
└─# cat user.txt
dd58ce67b49e15105e88096c8d9255a5

┌──(root💀kali)-[~/Downloads]
└─#
```

Enum FTP for port 80 credentials

```
ftp> ls -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16  10:46PM       <DIR>          $RECYCLE.BIN
02-03-19  12:18AM                 1024 .rnd
11-20-16  09:59PM               389408 bootmgr
07-16-16  09:10AM                    1 BOOTNXT
02-03-19  08:05AM       <DIR>          Documents and Settings
02-25-19  10:15PM       <DIR>          inetpub
06-18-21  02:14PM            738197504 pagefile.sys
07-16-16  09:18AM       <DIR>          PerfLogs
02-25-19  10:56PM       <DIR>          Program Files
02-03-19  12:28AM       <DIR>          Program Files (x86)
02-25-19  10:56PM       <DIR>          ProgramData
02-03-19  08:05AM       <DIR>          Recovery
02-03-19  08:04AM       <DIR>          System Volume Information
02-03-19  08:08AM       <DIR>          Users
02-25-19  11:49PM       <DIR>          Windows
226 Transfer complete.
ftp>
```

```
ftp> ls -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  08:05AM       <DIR>          Application Data
02-03-19  08:05AM       <DIR>          Desktop
02-03-19  08:05AM       <DIR>          Documents
02-03-19  12:15AM       <DIR>          Licenses
11-20-16  10:36PM       <DIR>          Microsoft
02-03-19  12:18AM       <DIR>          Paessler
02-03-19  08:05AM       <DIR>          regid.1991-06.com.microsoft
07-16-16  09:18AM       <DIR>          SoftwareDistribution
02-03-19  08:05AM       <DIR>          Start Menu
02-03-19  12:15AM       <DIR>          TEMP
02-03-19  08:05AM       <DIR>          Templates
11-20-16  10:19PM       <DIR>          USOPrivate
11-20-16  10:19PM       <DIR>          USOShared
02-25-19  10:56PM       <DIR>          VMware
```

```
226 Transfer complete.
ftp> cd Desktop
550 Access is denied.
ftp> cd Documents
550 Access is denied.
ftp> cd Paessler
250 CWD command successful.
ftp> ls -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
06-18-21  02:57PM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd PRTG\ Network\ Monitor
250 CWD command successful.
```

These files are most likely containing credentials

```
125 Data connection already open; Transfer starting.
06-18-21  02:57PM       <DIR>          Configuration Auto-Backups
06-18-21  02:15PM       <DIR>          Log Database
02-03-19  12:18AM       <DIR>          Logs (Debug)
02-03-19  12:18AM       <DIR>          Logs (Sensors)
02-03-19  12:18AM       <DIR>          Logs (System)
06-18-21  02:15PM       <DIR>          Logs (Web Server)
06-18-21  02:20PM       <DIR>          Monitoring Database
02-25-19  10:54PM              1189697 PRTG Configuration.dat
02-25-19  10:54PM              1189697 PRTG Configuration.old
07-14-18  03:13AM              1153755 PRTG Configuration.old.bak
06-18-21  02:57PM              1670275 PRTG Graph Data Cache.dat
02-25-19  11:00PM       <DIR>          Report PDFs
02-03-19  12:18AM       <DIR>          System Information Database
02-03-19  12:40AM       <DIR>          Ticket Database
02-03-19  12:18AM       <DIR>          ToDo Database
```

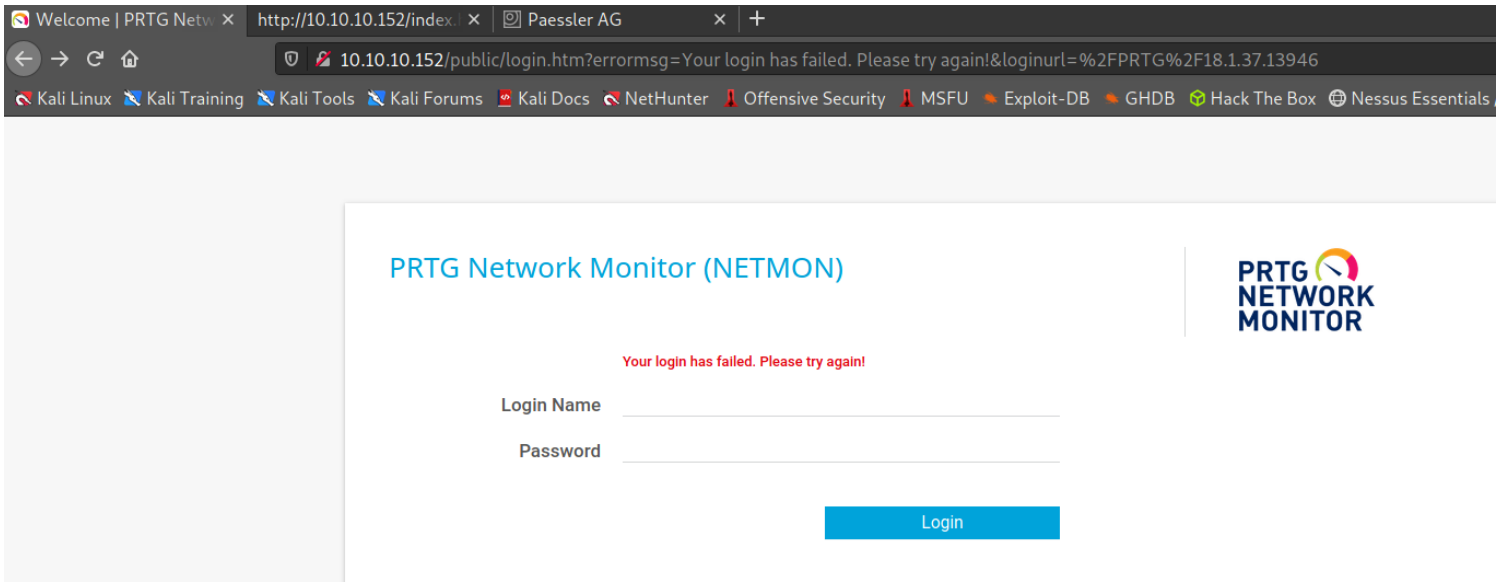
Download and inspect

```
    <encrypted/>
  </flags>
</comments>
<dbauth>
  0
</dbauth>
<dbcredentials>
  0
</dbcredentials>
<dbpassword>
  <!-- User: prtgadmin -->
  PrTg@dmin2018
</dbpassword>
<dbtimeout>
  60
</dbtimeout>
<depdelay>
  0
```

password 1 of 246
Match Case
Match Entire Word Only
Match as Regular Expression
Wrap Around

Port 80

80/tcp open http Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)



→ try with default credentials prtgadmin:prtgadmin ⇒ **FAILED**